Cybersecurity in Health Systems

Digital Threats, Real-World Consequences

Mitchell Sorensen, PharmD, PGY2 Pharmacy Informatics Resident, ASLMC

Date: 5/14/26

Disclosures

The planner(s) and speaker(s) have indicated that there are no relevant financial relationships with any ineligible companies to disclose.

Learning Objectives

At the end of this session, learners should be able to:

- Identify common methods for cyberattacks
- Summarize the means health organizations can use to mitigate cyber risks
- List cybersecurity best practices for healthcare teammates
- Distinguish the risks and benefits of artificial intelligence in cybersecurity

Outline

- Background of Cybersecurity
  - Cyberattack methods
  - Methods of attack prevention
- Case Studies
- Promoting cybersecurity at a user level
- Artificial Intelligence in Cybersecurity

Abbreviation Key

- AI: Artificial Intelligence
- ACK: Acknowledge
- CVE: Common Vulnerabilities and Exposures
- DDoS: Distributed-Denial-of-Service
- DoS: Denial-of-Service
- EHR: Electronic Health Record
- HTTPS: Hypertext Transfer Protocol Secure
- ID: Identification
- IDS: Intrusion Detection System
- IoT: Internet of Medical Things
- IP: Internet Protocol
- LLM: Large Language Model
- MAR: Medication Administration Record
- MFA: Multi-Factor Authentication
- MitM: Man-in-the-Middle
- PA: Prior Authorization
- RaaS: Ransomware-as-a-Service
- SYN: Synchronize
- SYN-ACK: Synchronize-acknowledge
- SIEM: Security Information and Event Management
- VPN: Virtual Private Network

Background of Cybersecurity

ADVOCATE HEALTH

Definitions

Cybersecurity:

- The practice of protecting systems, networks, devices, and data from digital attacks

Cyber-attack:

- A malicious and purposeful attempt to breach an individual's or organization's information system

Cisco. What is cybersecurity? 2025.
Cisco. What is a cyberattack? 2025.

Healthcare Cyberattack Motives

- Healthcare is an easy target
  - Healthcare IT environments are complex which can be difficult to secure
  - Old devices and software are vulnerable
- Healthcare systems store large amounts of valuable data
  - Social security numbers and other demographics for identity fraud
  - Sensitive medical information can be used for extortion

ADVOCATE HEALTH

HIPAA Journal. Why do criminals target medical records? 2026.

Targets

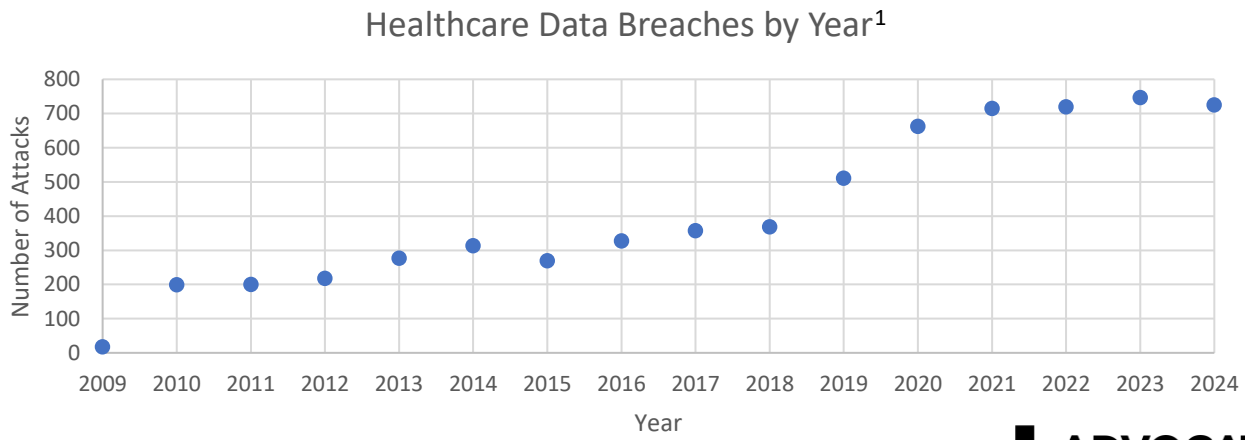
- Electronic Health Record (EHR)
- Internet of Medical Things (IoMT)
  - Infusion Pump
  - Imaging
    - MRI machine
    - CT scanner
    - X-ray machine
  - Implants
    - ICD
    - Pacemaker
  - Glucometer
  - Insulin Pump

ADVOCATE HEALTH

Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. 2024.

Cyberattack Statistics

- Number of healthcare data breaches has been steadily increasing each year
  - From 18 attacks in 2009 to 725 attacks reported in 2024
    - Involving breaches of 500 or more records

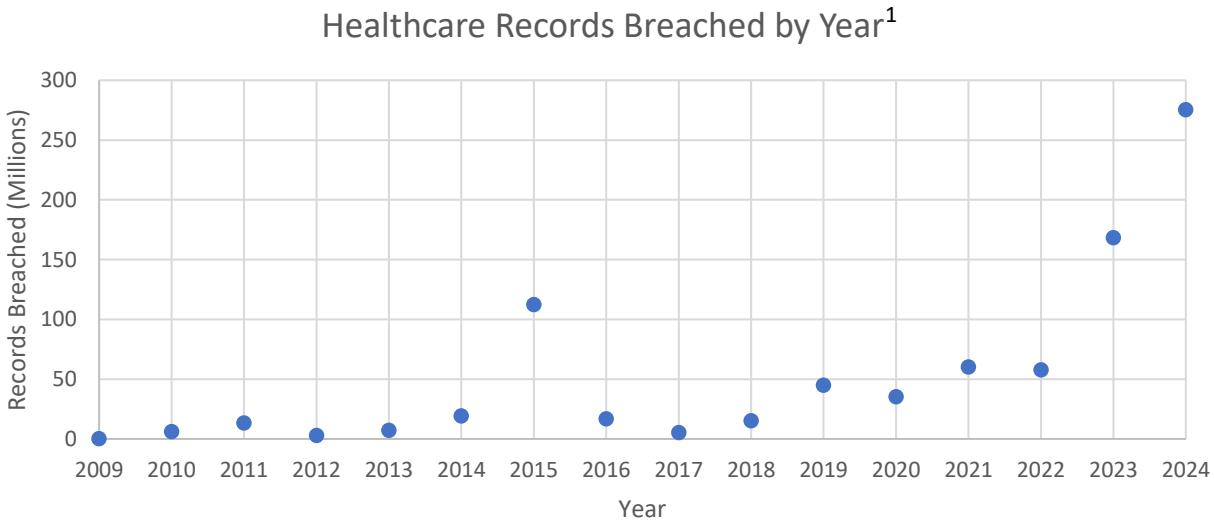


ADVOCATE HEALTH

HIPAA Journal. 2024 healthcare data breach report. 2025.

Cyberattack Statistics

- Number of records breached each year has been increasing rapidly

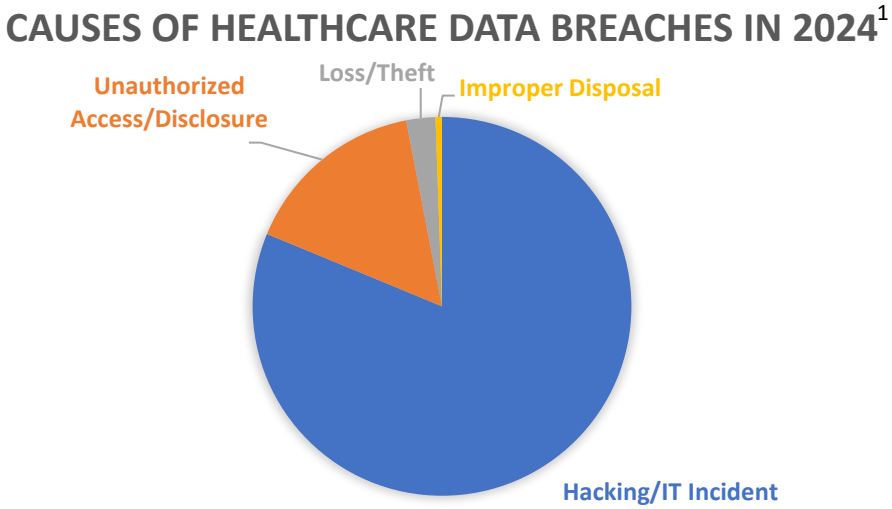


ADVOCATE HEALTH

HIPAA Journal. 2024 healthcare data breach report. 2025.

Cyberattack Statistics

- Majority of healthcare data breaches are due to hacking/IT incidents



ADVOCATE HEALTH

HIPAA Journal. 2024 healthcare data breach report. 2025.

Types of Cyberattacks

ADVOCATE HEALTH

Malware

- Definition: Malicious software made to harm, disrupt, or gain unauthorized access to systems
- Ransomware: Malware that locks down files or systems and demands payment to restore access
- Spyware: Malware that covertly tracks user activity
- Viruses: self-replicating software that requires a host program to run to make it active
- Worms: self-propagating program that independently runs that can consume computer resources destructively
- Trojans: Seemingly useful program but with a hidden and possibly malicious function

Cisco. What is a cyberattack? 2025.
NIST. Virus. 2026.
NIST. Worm. 2026.
NIST. Trojan horse. 2026.

Phishing

- Definition: Social engineering technique to obtain sensitive data through fraudulent solicitation via an email or website
  - The solicitation often imitates legitimate businesses or a reputable person
- One of the means that malware is introduced into a system

ADVOCATE HEALTH

NIST. Phishing. 2026.

Man-in-the-Middle (MitM)

- Definition: Attacker places themselves between two communicating targets to steal sensitive information or alter information being sent
  - Between two users
  - Between a user and an application
- Entry points for attacker
  - Phishing attacks
  - Public Wi-Fi hotspots
    - Fewer security protocols

ADVOCATE HEALTH

IBM. What is a man-in-the-middle attack? 2026.

Denial-of-Service (DoS)

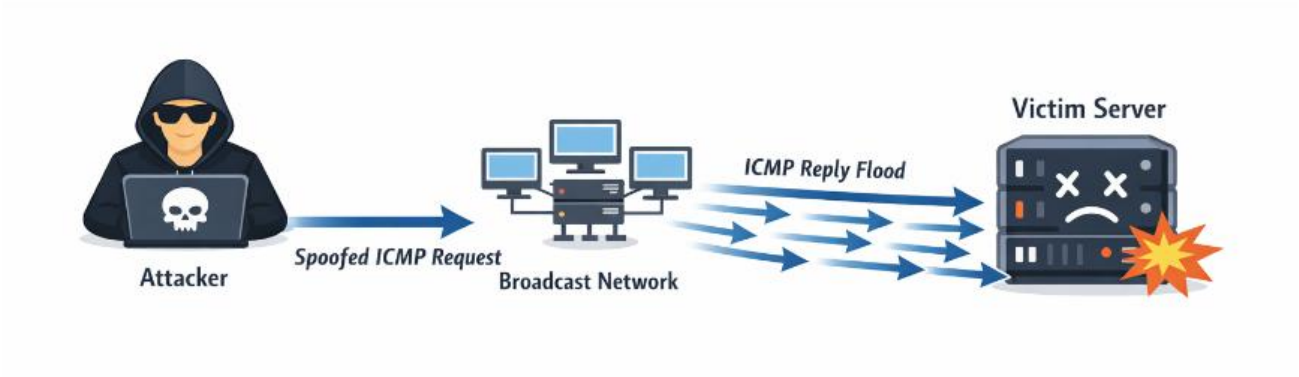
- Definition: Attack that renders a targeted host or network unusable due to being flooded with traffic
  - Distributed Denial-of-Service (DDoS):
    - Subtype of DoS where the attack occurs with multiple machines operating together
    - Often uses a botnet
      - Network of compromised devices
    - Increases attack power

ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- Smurf Attack:
  1. Attacker spoofs a target's IP address and sends internet control message protocol broadcast packets (pings) to numerous hosts
  2. Hosts reply to the target's IP address (flooding it with responses)



ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

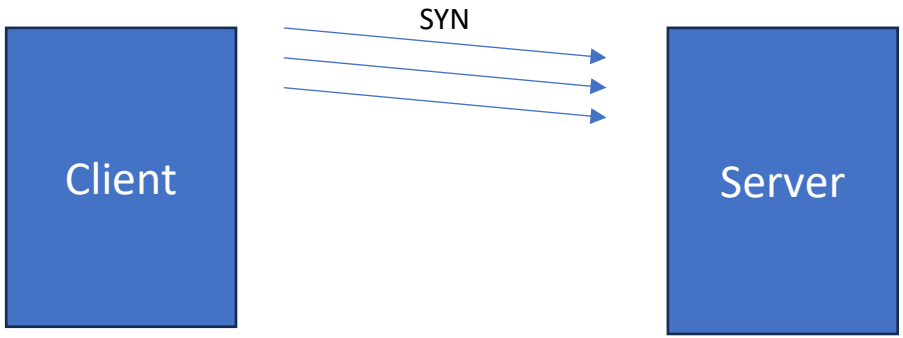
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

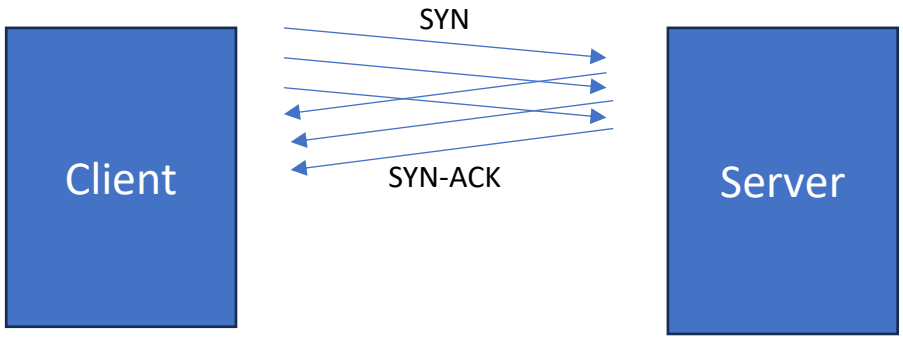


ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

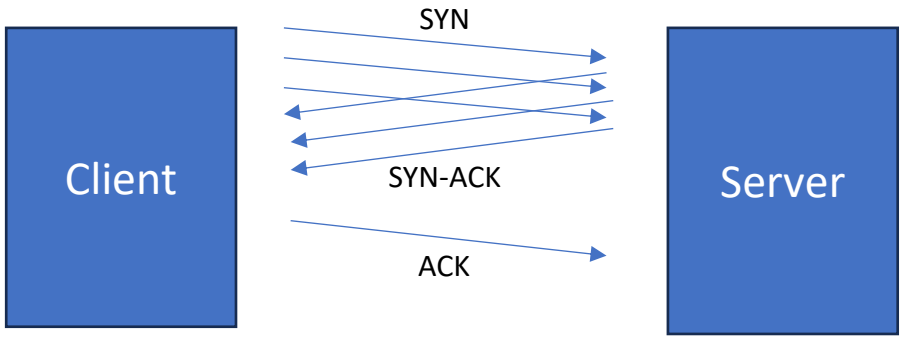


ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

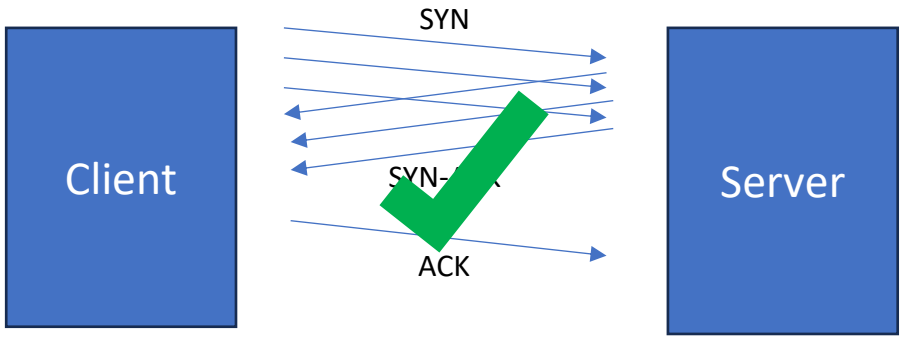


ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

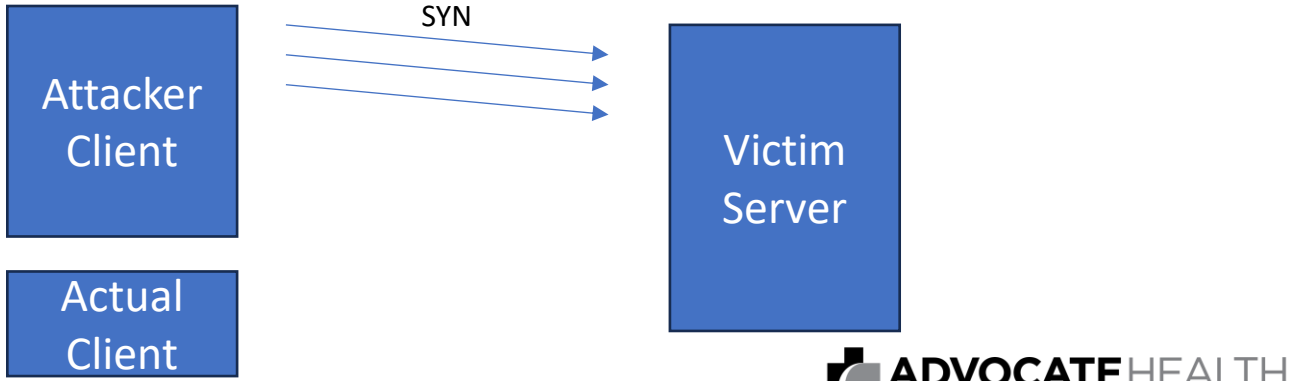
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

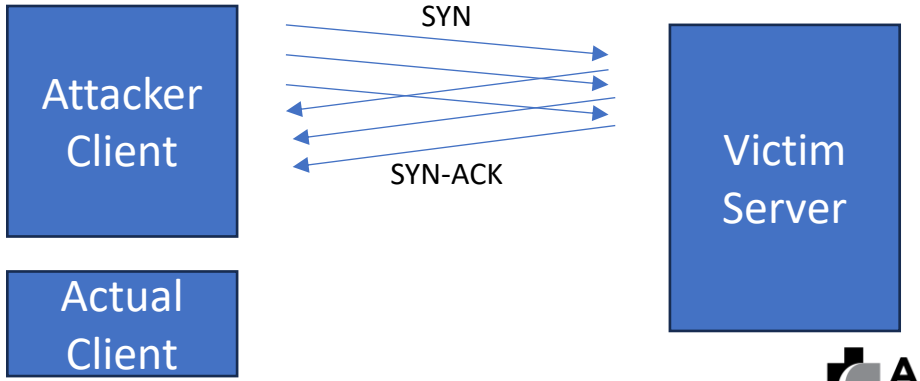
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect

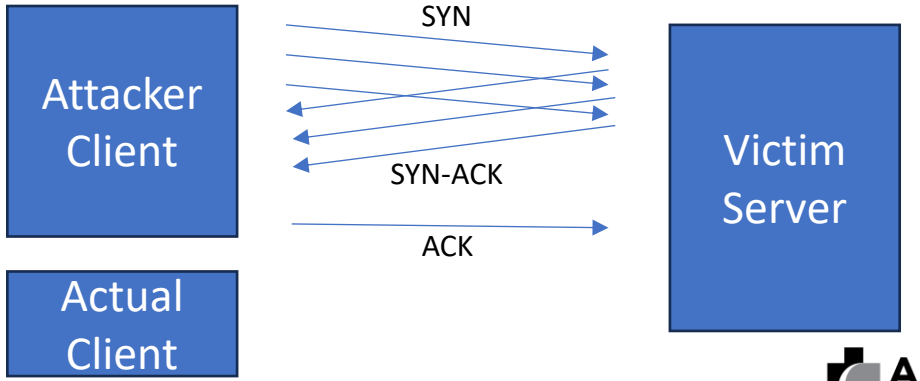


ADVOCATE HEALTH

CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

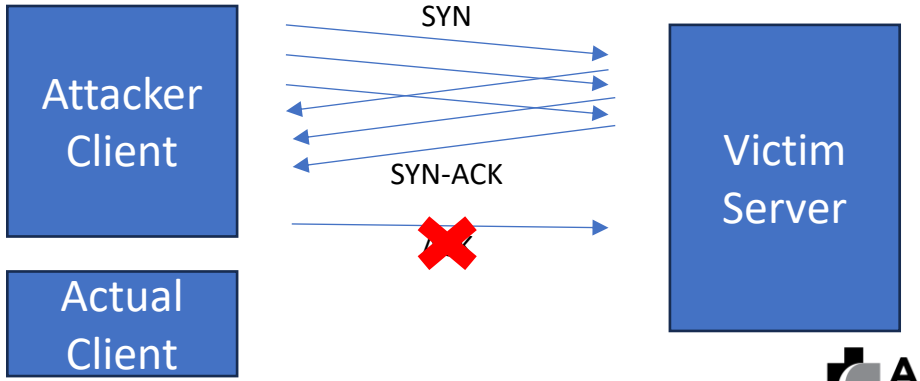
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

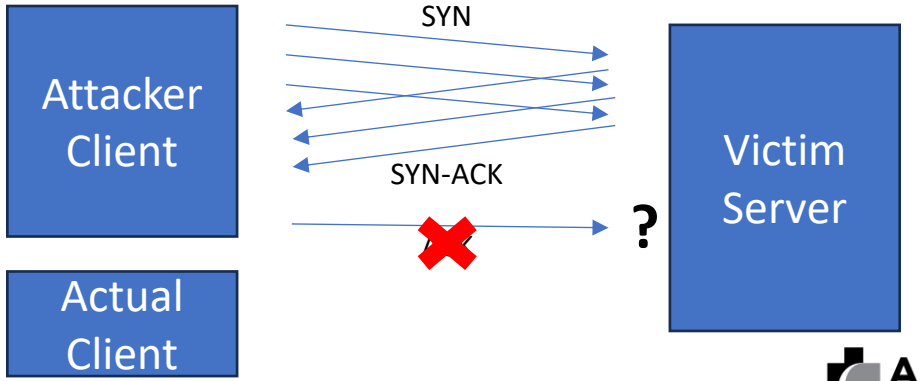
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

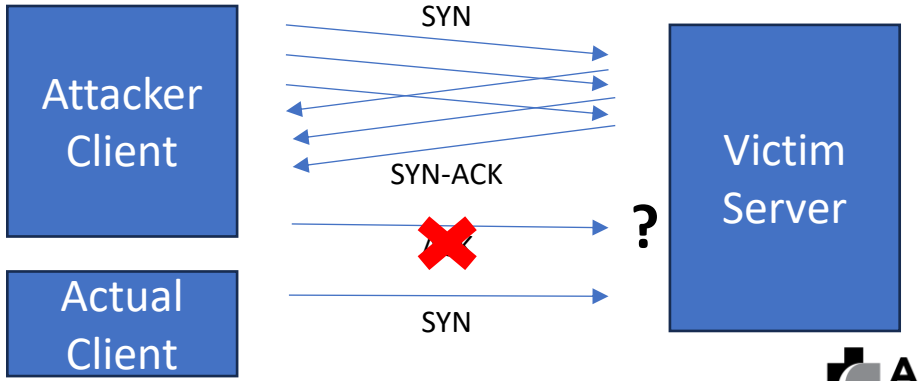
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

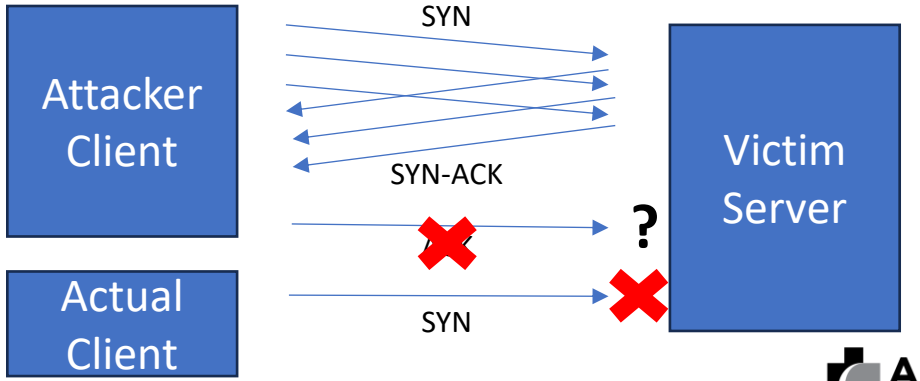
- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Denial-of-Service

- SYN Flood
  - Attacker sends a request to connect to a targeted server but does not complete the “three-way handshake” to create a connection
    - Attacker repeats this process to saturate connection ports
  - The incomplete handshake leaves the connected port in an occupied status so other legitimate users can’t connect



CISA. Understanding denial-of-service attacks. 2026.

Login Attacks

- Brute Force Attack: Uses automation to systematically try passwords for a user ID until the correct one is entered
- Password Spraying: Attempts one common passwords across many accounts
- Password Stuffing: Uses stolen login combinations across multiple sites

ADVOCATE HEALTH

CrowdStrike. What is a brute force attack? 2026.

Assessment Question #1

What type of cyberattack relies on not completing a “three-way handshake” to establish a connection to a server?

A. Smurf Attack
B. SYN Flood
C. Phishing
D. Man-in-the-Middle

Combating Cyberattacks

ADVOCATE HEALTH

Internal Controls

- Preventative
  - Stops an incident before it happens
- Detective
  - Identifies an incident during or soon after an attack
- Corrective
  - Reduces the impact of an incident and restores operations

ADVOCATE HEALTH

CyberQuizzer. Preventive, detective, and corrective controls. 2025.

Preventative Controls

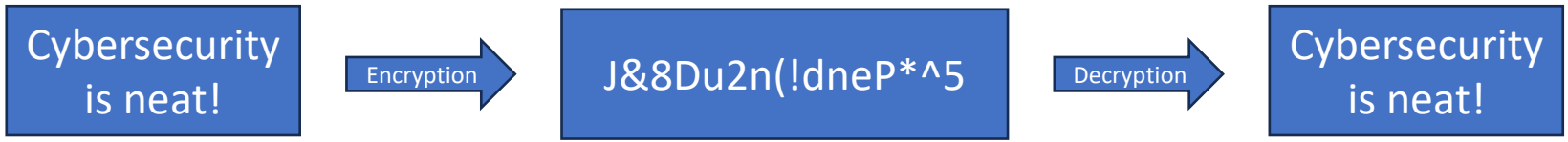
- Firewall
  - Security device that monitors and filters incoming and outgoing network traffic
    - External threats: viruses, phishing emails, DoS attacks
    - Internal threats: exfiltration of data
  - Serves as a barrier between external networks and a trusted internal network

ADVOCATE HEALTH

Fortinet. Firewall. 2026.

Preventative Controls

- Encryption
  - Information is converted to an unreadable text (ciphertext) so it is useless to unauthorized users
  - Authorized users can decipher the text

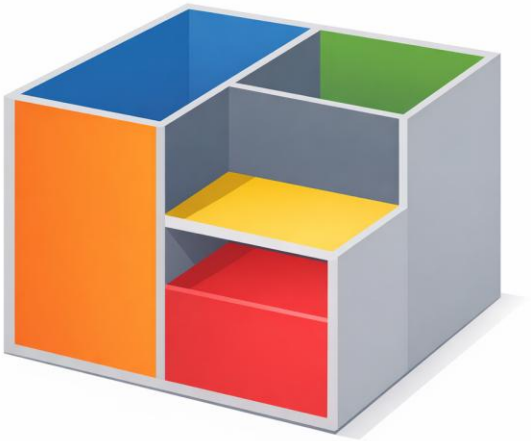


ADVOCATE HEALTH

Fortinet. Encryption. 2026.

Preventative Controls

- Network Segmentation
  - Divides a computer network into smaller isolated sections to restrict communication
  - Can limit the spread of an attack
    - One segment does not automatically give access to another
  - Example: Segmenting ADS cabinets, infusion pumps, payroll, and email from each other



GeeksforGeeks. What is network segmentation? 2026.

ADVOCATE HEALTH

Preventative Controls

- Principle of Least Privilege (PoLP)
  - Concept of granting users the minimum level of access to perform their duties
    - Reduces the risk of both accidental or intentional misuse of information
- Update software regularly
  - Software can contain security flaws
  - Vendors release patches once flaws are identified
  - When patches are released, the security vulnerabilities may become public knowledge
    - Attackers can reverse engineer the patches to create exploits for systems that haven't been updated

Fortinet. Principle of least privilege, 2026.
Kukoyi M. Software updates and patches, 2024.

Detective Controls

- Antivirus
  - Scans and detects malware on a device
  - Types of Detection
    - Signature-based: scan looks for known malware signatures from a database
      - Fast and low false positives
    - Behavior-based: continuous monitoring that analyzes process abnormalities
      - Can require more processing power and higher false positives

ADVOCATE HEALTH

SentinelOne. Signature-based vs behavioral AI detection. 2026.

Detective Controls

- Intrusion Detection Systems (IDS)
  - Application that monitors network or system activity and identifies suspicious or malicious activity
  - Types of IDS
    - Network IDS: Monitors incoming and outgoing traffic from all devices connected to an organization's network
    - Host-based IDS: Monitors activity on an individual host connected to the internet/organization's intranet

ADVOCATE HEALTH

Fortinet. Intrusion detection system (IDS). 2026.

Detective Controls

- Security Information and Event Management (SIEM)
  - Centralized cybersecurity system that
    - Collects and analyzes security events from different sources across an organization
      - Antivirus
      - Intrusion Detection System
      - Identity and Access Management Tools
      - Email Security Tools
    - Alerts security team as needed

ADVOCATE HEALTH

Behl A, Behl K. Cybersecurity detective controls. 2015.

Corrective Controls

- Wide variety of examples
  - Investigating how an incident occurred to help close possible cybersecurity defense gaps
  - Software patch
  - Restoring systems from backups
  - Education to end users
  - Revised policies and mitigation strategies

ReasonLabs. Corrective controls. 2026.
ScienceInsights. What is a corrective control? 2026.

Assessment Question #2

A health system identified that a server was compromised due to a software vulnerability. The health system's IT security team removed the server from the network and resolved the vulnerability with a software patch before restoring access. What type of cybersecurity control is primarily demonstrated by the actions taken by the IT security team?

A. Preventative Control
B. Detective Control
C. Corrective Control

Healthcare Teammate Cybersecurity Best Practices

ADVOCATE HEALTH

Best Practices

- Use strong passwords
  - At least 16 characters long
  - Mix of upper and lowercase letters, numbers, and symbols
  - Only use for one account
- Use caution while on public WiFi
  - Attackers can access and compromise sensitive information
  - Ensure websites start with http**s**
  - Consider using a VPN

CISA. Require strong passwords. 2026.
FCC. How to protect yourself online. 2026.

ADVOCATE HEALTH

Best Practices

- Multi-Factor Authentication (MFA)
  - Method of verifying identify by requiring at least two proofs
  - Factors include:
    - Something you know (e.g. password)
    - Something you have (e.g. mobile phone)
    - Something you are (e.g. biometric)
- Backup Data
  - Prevent data loss due to a cyberattack
  - Follow the 3-2-1 rule
    - 3 copies of important files
    - 2 different types of storage
    - 1 copy stored off site

IBM. What is multi-factor authentication? 2026.
NIST. Multi-factor authentication. Updated 2026.
CISA. Back up business data. 2026.

ADVOCATE HEALTH

Best Practices

- Be aware of phishing
  - Review phishing educational materials
  - Look for suspicious e-mails, text messages, or voice calls
    - Communications that imply urgency or request unusual tasks be completed
  - Validate the source through alternate means of communication
  - Report identified malicious communications

ADVOCATE HEALTH

U.S. Dep't of State. Understanding and preventing phishing attacks. 2026.

Best Practices

- Be prepared for downtimes
  - Know your health system's downtime procedures
  - Practice downtime workflow drills
  - Prepare for the loss of medication safeguards
  - Know alternate means of communication

ADVOCATE HEALTH

AMC PSO. Patient safety guidance for EHR downtime. 2017.

Assessment Question #3

Mike logs into his email first by entering his password and then by scanning his fingerprint. Which of the following is NOT a type of factor Mike used when performing this example of MFA?

A. Something you know
B. Something you have
C. Something you are

Case Studies

ADVOCATE HEALTH

Change Healthcare: 2024

Background

- Victim: Change Healthcare, a healthcare clearing house and a subsidiary of United Health Group
- Attacker: Individuals associated with BlackCat ransomware group
  - Ransomware-as-a-Service (RaaS) group
- Attack:
  - Infiltrated the network through a remote access Citrix portal that lacked MFA
  - BlackCat exfiltrated large amounts of data then deployed ransomware

Security.org. Change Healthcare data breach. 2026.
HIPAAGuide. Change Healthcare data breach. 2025.

ADVOCATE HEALTH

Change Healthcare: 2024

Outcome

- Change Healthcare shut down systems to prevent further spread
- Paid $22 million ransom to BlackCat in exchange that the data would be deleted
- Over 190 million individuals affected
- Total impact of over $3 billion on UnitedHealth Group

Lessons Learned

- Utilize MFA
- Update system regularly

Security.org. Change Healthcare data breach. 2026.
HIPAAGuide. Change Healthcare data breach. 2025.

ADVOCATE HEALTH

Lurie Children's Hospital: 2024

Background

- Victim: Lurie Children's Hospital in Chicago, IL
- Attacker: Rhysida
  - RaaS group
- Attack
  - Method of attack is not public but some suspect it was due to an outdated identification system
  - Accessed patient data and deployed ransomware

CISA. #StopRansomware: Change Healthcare advisory (AA23-319A). 2023.
HIT Consultant. Legacy Active Directory ransomware risks. 2026.
HIPAA Journal. Lurie Children's Hospital cyberattack. 2024.

ADVOCATE HEALTH

Lurie Children's Hospital: 2024

Outcome

- Forced IT systems offline
  - Reverted to downtime workflows for several months
- Over 790,000 individuals affected
- Rhysida demanded a $3.4 million ransom
  - Not paid
  - Group claims to have sold the patient data

Lessons Learned

- Keep systems updated

CISA. #StopRansomware: Change Healthcare advisory (AA23-319A). 2023.
HIT Consultant. Legacy Active Directory ransomware risks. 2026.
HIPAA Journal. Lurie Children's Hospital cyberattack. 2024.

ADVOCATE HEALTH

Ascension Health: 2024

Background

- Victim: Ascension Health
  - One of the largest nonprofit health systems in the nation
- Attacker
  - Believed to be the Black Basta ransomware group
    - RaaS group
- Attack
  - Employee inadvertently downloaded a malicious file
  - Ransomware was used to encrypt files

CISA. #StopRansomware: Black Basta (AA24-131A). 2024.
HIPAA Journal. Ascension cyberattack. 2024.

ADVOCATE HEALTH

Ascension Health

Outcome

- Patient data stolen affecting 5.6 million individuals
- Critical systems were taken offline for ~6 weeks
- Forced ambulances to be diverted and for pharmacies to close
- Contributed to their $1.1 billion net loss in the 2024 fiscal year

Lessons learned

- Educate staff about cybersecurity

CISA. #StopRansomware: Black Basta (AA24-131A). 2024.
HIPAA Journal. Ascension cyberattack. 2024.

ADVOCATE HEALTH

Artificial Intelligence (AI) in Cybersecurity

ADVOCATE HEALTH

AI in Cybersecurity

- AI: An umbrella term to describe the ability of a computer system to perform tasks typically requiring human intelligence
- Generative AI: Creates new patterns and content
  - Relies on prompts
  - Large Language Model (LLM): Subset of genAI that understand and generate human language
- Agentic AI: Reasons and makes decisions autonomously
  - Doesn’t require human prompts

ADVOCATE HEALTH

IBM. Agentic AI vs generative AI. 2026.

AI in Cybersecurity

- Threat detection
  - Detects abnormal behavior by learning users' typical behavior
    - Login patterns
    - File access histories
    - Application usage
    - Network activity
  - Traditional systems are based on rules

ADVOCATE HEALTH

Mohamed N. AI and machine learning in cybersecurity. 2025.

AI in Cybersecurity

- Malware Detection
  - Can identify malware based on learning patterns from malware signatures
  - Able to better identify polymorphic malware
- Phishing Detection
  - Can identify if a communication is phishing based on patterns found in phishing databases
    - Can recognize linguistic cues that indicate malicious intent

ADVOCATE HEALTH

Mohamed N. AI and machine learning in cybersecurity. 2025.

AI in Cybersecurity

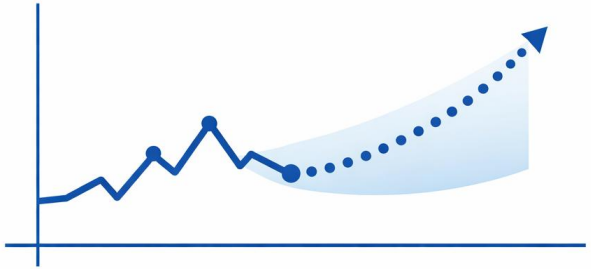
- Automation
  - Traditional cybersecurity involves manual workflows
  - Traditional SIEM systems often struggle with high data volume and false positive rates
    - AI can review logs and filter out false positives
  - AI-detected compromises can automatically trigger predefined response actions
    - Reduces mean time to detect and respond

Mohamed N. AI and machine learning in cybersecurity. 2025.
Roy S. AgenticCyber multi-agent cybersecurity system. 2025.

ADVOCATE HEALTH

AI in Cybersecurity

- Proactive Decision Making
  - AI can forecast possible threats and vulnerabilities using predictive analytics before they are exposed by attackers
  - AI can help identify possible system exploitations and ranks its severity
  - Allows organizations to continuously strengthen their security capabilities



ADVOCATE HEALTH

Mohamed N. AI and machine learning in cybersecurity. 2025.

Risks of AI in Cybersecurity

ADVOCATE HEALTH

AI in Cybersecurity: Risks

- Although AI is an effective tool it does have limitations/risks associated with its use
  - Bias: AI is only as good as the data it's trained on
  - Transparency: AI is complex which can sometimes make it difficult to understand how it came to certain decisions
    - "Black Box" AI

ADVOCATE HEALTH

GeeksforGeeks. AI in cybersecurity. 2025.

AI in Cybersecurity: Risks

- Privacy Concerns
  - Cybersecurity using AI typically involves collecting and analyzing large amounts data
- AI Powered Attacks
  - Hackers can utilize AI as a tool to attack more efficiently

ADVOCATE HEALTH

Guembe B et al. AI-driven cyber attacks. 2022.

AI Attacks: Logins

- Brute-Force AI
  - Utilizes an AI agent alongside an LLM to identify login pages
    - Agent sends webpages to LLM which scans the page for login fields
  - Attack
    - Brute Force
    - Password Spraying

Guembe B et al. AI-driven cyber attacks. 2022.

ADVOCATE HEALTH

AI Attacks: Phishing

- Attackers can give an LLM prompts to generate phishing attacks
  - Rate of phishing attack creation is faster
  - AI can eliminate signs of a phish
    - Grammatical and spelling errors
    - Unusual tone
  - Attacks are more believable
    - Tailored to individual recipients
    - Mimic linguistic style of the individual

Sami M, et al. Computational models for sign language recognition. 2023.
Kumar S, Menezes A, Giri S, Kotikela S. What the phish! Effects of AI on phishing attacks and defense. 2024.

AI Attacks: Deepfakes

- AI generated media (e.g. pictures, audio, video) impersonating an individual doing something never actually done
- Attackers can
  - Feed generative AI media of an individual to impersonate
  - Give AI a script to perform
  - Send the deepfake to victims

Deepfake of Morgan Freeman that I have generated

ADVOCATE HEALTH

Dash B, Sharma P. Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? 2023.

AI Attacks: Ransomware

- PromptLock
  - Proof of concept only
- AI agent alongside an LLM to perform all aspects of a ransomware attack
  - Identifies what systems/organizations to attack
  - Analyzes what data is sensitive and valuable
  - Deploys the attack
  - Writes the ransom note

ADVOCATE HEALTH

ESET Research. AI-powered ransomware (PromptLock). 2025.

AI Attacks: CVE Exploits

- Common Vulnerabilities and Exposures: Publicly disclosed security vulnerability reports
- Attackers can use AI tools like “CVE-Genie” (AI agent) to
  - Feed CVEs to an LLM to read and send back pertinent information back to the agent
  - Have the AI agent understand the vulnerability and write an exploit

ADVOCATE HEALTH

Ullah S, et al. Automated multi-agent framework for reproducing CVEs. 2026.

AI Attacks: Cases

- United Kingdom engineering firm Arup tricked into sending $25 million to fraudsters - 2024
  - Employee transferred money following a video call with senior management
- Anthropic (Claude) AI powered cyber espionage campaign - 2025
  - Chinese state-sponsored group used Claude code to:
    - Support reconnaissance, vulnerability discovery, exploitation, credential harvesting, data analysis and exfiltration
    - Execute 80-90% of the tactical operations independently

World Economic Forum. Deepfake-enabled cybercrime (Arup case). 2025.
Anthropic. Disrupting the first reported AI-orchestrated cyber espionage campaign. 2025.

Assessment Question #4

Which of the following correctly distinguishes the risks and benefits of AI in cybersecurity?

A. AI can increase efficiency by filtering out false positive threats, but may introduce bias if models are trained on poor quality data

B. AI can automate incident response, but slows down response times

C. AI prevents all cyber attacks, but raises privacy concerns

D. AI always identifies threats correctly, but its decision-making process may lack transparency

Summary/Conclusion

- Cyberattacks are a growing threat in healthcare
- Attacks can affect more than an EHR
- There are a variety of attack methods
- Preventative, detective, and corrective controls are used to combat cyberattacks
- AI enhances cybersecurity but comes with risks

Questions?

Mitchell Sorensen, PharmD
mitchell.sorensen@aah.org

References

1. Cisco. What is cybersecurity? Cisco. Published 2025. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html
2. Cisco Systems Inc. What is a cyberattack? Cisco. Accessed April 12, 2026. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html
3. HIPAA Journal. Why do criminals target medical records? HIPAA Journal. Published January 10, 2026. Accessed April 12, 2026. https://www.hipaajournal.com/why-do-criminals-target-medical-records/
4. Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. Healthc Manage Forum. 2024;37(1):17-20. doi:10.1177/08404704231195804
5. HIPAA Journal. 2024 healthcare data breach report. HIPAA Journal. Published January 30, 2025. Accessed April 12, 2026. https://www.hipaajournal.com/2024-healthcare-data-breach-report/
6. National Institute of Standards and Technology (NIST). Virus. NIST Computer Security Resource Center. Accessed April 12, 2026. https://csrc.nist.gov/glossary/term/virus
7. National Institute of Standards and Technology (NIST). Worm. NIST Computer Security Resource Center. Updated 2026. Accessed April 12, 2026. https://csrc.nist.gov/glossary/term/worm
8. National Institute of Standards and Technology (NIST). Trojan horse. NIST Computer Security Resource Center. Updated 2026. Accessed April 12, 2026. https://csrc.nist.gov/glossary/term/trojan_horse
9. National Institute of Standards and Technology (NIST). Phishing. NIST Computer Security Resource Center. Updated 2026. Accessed April 12, 2026. https://csrc.nist.gov/glossary/term/phishing
10. IBM Corporation. What is a man-in-the-middle attack? IBM. Accessed April 12, 2026. https://www.ibm.com/think/topics/man-in-the-middle

References

11. U.S. Cybersecurity and Infrastructure Security Agency (CISA). Understanding denial-of-service attacks. CISA. Accessed April 12, 2026.https://www.cisa.gov/news-events/news/understanding-denial-service-attacks
12. CrowdStrike Inc. What is a brute force attack? CrowdStrike. Accessed April 12, 2026. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/brute-force-attack/
13. CyberQuizzer. Preventive, detective, and corrective controls: a complete guide. CyberQuizzer. Published August 11, 2025. Accessed April 12, 2026.https://www.cyberquizzer.com/blog/preventive-detective-corrective-controls
14. Fortinet Inc. Firewall. Fortinet. Accessed April 12, 2026. https://www.fortinet.com/resources/cyberglossary/firewall
15. Fortinet Inc. Encryption. Fortinet. Accessed April 12, 2026. https://www.fortinet.com/resources/cyberglossary/encryption
16. GeeksforGeeks. What is network segmentation? GeeksforGeeks. Published April 17, 2023. Accessed May 2, 2026. https://www.geeksforgeeks.org/computer-networks/what-is-network-segmentation/
17. Fortinet. What is the principle of least privilege (PoLP)? Fortinet Cyber Glossary. Accessed May 2, 2026.https://www.fortinet.com/resources/cyberglossary/principle-of-least-privilege
18. Kukoyi M. The importance of regular software updates and patches. IT Security Insights. Published June 26, 2024. Accessed May 2, 2026.https://www.itsecurityinsights.com/the-importance-of-regular-software-updates-and-patches/
19. SentinelOne. Signature-based vs behavioral AI detection. SentinelOne. Accessed April 12, 2026. https://www.sentinelone.com/cybersecurity-101/cybersecurity/signature-based-vs-behavioral-ai-detection/
20. Fortinet Inc. Intrusion detection system (IDS). Fortinet. Accessed April 12, 2026. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

References

21. Behl A, Behl K. Cybersecurity detective controls: monitoring to identify and respond to threats. ISACA J. 2015;5.
22. ReasonLabs. Corrective controls. Cyberpedia. Accessed April 12, 2026. https://cyberpedia.reasonlabs.com/EN/corrective%20controls.html
23. ScienceInsights. What is a corrective control? Definition and examples. ScienceInsights. Published March 21, 2026. Accessed April 12, 2026.https://scienceinsights.org/what-is-a-corrective-control-definition-and-examples/
24. U.S. Cybersecurity and Infrastructure Security Agency (CISA). Require strong passwords. CISA. Accessed April 12, 2026.https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-strong-passwords
25. Federal Communications Commission (FCC). How to protect yourself online. FCC. Accessed April 12, 2026.https://www.fcc.gov/consumers/guides/how-protect-yourself-online
26. IBM Corporation. What is multi-factor authentication? IBM. Accessed April 12, 2026. https://www.ibm.com/think/topics/multi-factor-authentication
27. National Institute of Standards and Technology (NIST). Multi-factor authentication (MFA). NIST Computer Security ResourceCenter. Updated 2026. Accessed April 12, 2026. https://csrc.nist.gov/glossary/term/Multi_Factor_Authentication
28. U.S. Cybersecurity and Infrastructure Security Agency (CISA). Back up business data. CISA. Accessed April 12, 2026.https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/back-up-business-data
29. U.S. Department of State. Understanding and preventing phishing attacks. U.S. Department of State. Accessed April 12, 2026.https://www.state.gov/understanding-and-preventing-phishing-attacks/
30. Academic Medical Center Patient Safety Organization (AMC PSO). Patient safety guidance for electronic health record downtime:recommendations of the Electronic Health Record Downtime Task Force. Published 2017. Accessed April 9, 2026.https://flbog.sip.ufl.edu/wp-content/uploads/2019/11/AMC-PSO-EHR-Downtime.pdf

References

31. Security.org. Change Healthcare data breach. Security.org. Accessed April 12, 2026. https://www.security.org/identity-theft/breach/change-healthcare/

32. HIPAAGuide. Change Healthcare data breach. HIPAAGuide. Accessed April 12, 2026. https://www.hipaaguide.net/change-healthcare-data-breach/

33. U.S. Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware: Update on compromise of ChangeHealthcare. CISA Cybersecurity Advisory AA23-319A. Published November 15, 2023. Accessed April 12, 2026.https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a

34. HIT Consultant. How legacy Active Directory creates ransomware risks for hospitals. HIT Consultant. Published January 2, 2026.Accessed April 12, 2026. https://hitconsultant.net/2026/01/02/how-legacy-active-directory-creates-ransomware-risks-for-hospitals/

35. HIPAA Journal. January 2024 cyberattack on Lurie Children's Hospital affects 792,000 individuals. HIPAA Journal. PublishedJanuary 2024. Accessed April 12, 2026. https://www.hipaajournal.com/january-2024-cyberattack-on-lurie-childrens-hospital-affects-792k-individuals/

36. U.S. Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware: Black Basta. CISA Cybersecurity AdvisoryAA24-131A. Published May 10, 2024. Updated November 8, 2024. Accessed April 12, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

37. HIPAA Journal. Ascension cyberattack 2024. HIPAA Journal. Published 2024. Accessed April 12, 2026.https://www.hipaajournal.com/ascension-cyberattack-2024/

38. IBM Corporation. Agentic AI vs generative AI. IBM. Accessed April 12, 2026. https://www.ibm.com/think/topics/agentic-ai-vs-generative-ai

39. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and futureparadigms. Knowl Inf Syst. 2025;67:6969-7055. doi:10.1007/s10115-025-02429-y

40. Roy S. AgenticCyber: a GenAI-powered multi-agent system for multimodal threat detection and adaptive response incybersecurity. arXiv. 2025. arXiv:2512.06396v1. doi:10.48550/arXiv.2512.06396

ADVOCATE HEALTH

References

41. GeeksforGeeks. AI in cybersecurity. GeeksforGeeks. Updated August 6, 2025. Accessed April 12, 2026.https://www.geeksforgeeks.org/ethical-hacking/ai-in-cybersecurity/

42. Guembe B, Azeta A, Misra SN, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of AI-driven cyber attacks: areview. Appl Artif Intell. 2022;36(1):2037254. doi:10.1080/08839514.2022.2037254

43. Sami M, Tehseen R, Omer U, Khan MF, Siddiqui SY, Khan NS, Khan DA. Systematic literature review on computational modelsused for sign language recognition. J Comput Biomed Inform. 2023;8(1). https://www.jcbi.org/index.php/Main/article/view/567/534

44. Kumar S, Menezes A, Giri S, Kotikela S. What the phish! effects of AI on phishing attacks and defense. In: Proceedings of theInternational Conference on AI Research. Academic Conferences and Publishing International Ltd; 2024.

45. Dash B, Sharma P. Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. Int J Eng Appl Sci(IJEAS). 2023;10(1). Published January 2023. ISSN 2394-3661. Available at: https://www.ijeas.org

46. ESET Research. ESET discovers PromptLock, the first AI-powered ransomware. ESET Newsroom. Published August 27, 2025.https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware/

47. Ullah S, Balasubramanian P, Guo W, Burnett A, Pearce H, Kruegel C, Vigna G, Stringhini G. From CVE entries to verifiableexploits: an automated multi-agent framework for reproducing CVEs. arXiv. Published February 12, 2026. arXiv:2509.01835v2.Available at: https://arxiv.org/abs/2509.01835

48. World Economic Forum. Cybercrime: Lessons learned from a $25m deepfake attack. World Econ Forum. Published February 4,2025. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

49. Anthropic. Disrupting the first reported AI-orchestrated cyber espionage campaign. Anthropic; November 2025.https://www.anthropic.com/news/disrupting-AI-espionage